WHAT IS CLAIMED IS

1. A system for secure transmission of protected content, the system comprising:

a security server;

a recipient module; and

a secure communication channel for supporting communication between said security server and said recipient module,

wherein, in a first mode of operation, the recipient module receives a first key in a multiple key hierarchy via said secure channel, and

in a second mode of operation, the recipient module receives the protected content and an encrypted key, said encrypted key being a second key in said multiple key hierarchy, said recipient module being operative to utilize the first key to decrypt the encrypted key to form a decrypted key, said recipient module only being capable of accessing the protected content with said decrypted key.

2. The system of claim 1, wherein said first key is contained in a VEMM, said VEMM further comprising an access criteria reference for determining whether said recipient module is entitled to access the protected content and said VEMM being prepared by said security server.

3. The system of claim 2, wherein said access criteria reference for each item of protected content is associated with a separate access key.

4. The system of claim 2, wherein said encrypted key further comprises an encrypted control word.

5. The system of claim 4, wherein said encrypted control word is contained in a VECM, said VECM further comprising an access criteria reference for identifying said first key for decrypting said encrypted control word by said recipient module and said VECM being prepared by said security server.

6. The system of claim 5, wherein said secure communication channel further comprises a subscriber key, such that said first key is encrypted with said subscriber key for being transmitted to said recipient module, and such that said recipient module is capable of decrypting said subscriber key.

7. The system of claim 6, wherein said recipient module further comprises a secret, said secret being required for decrypting said subscriber key, and said secret comprising a part of said secure communication channel.

8. The system of claim 7, wherein said recipient module comprises at least one permanent read-only storage medium for storing said secret.

9. The system of claim 8, wherein said secret is permanently stored on said at least one permanent read-only storage medium during manufacture of said recipient module.

10. The system of claim 9, wherein said recipient module comprises at least one generic chip, said at least one generic chip comprising said at least one permanent read-only storage medium for storing said secret.

11. The system of claim 7, wherein said security server receives said subscriber key encrypted with said secret and an unencrypted subscriber key, but wherein said security server does not receive said secret.

12. The system of claim 7, further comprising a head-end for transmitting the protected content.

13. The system of claim 12, wherein said head-end sends a EMM to said security server, for providing said access criteria reference to said security server.

14. The system of claim 13, wherein said head-end sends at least information for generating said control word to said security server in an ECM.

15. The system of claim 14, wherein said head-end also sends said ECM to said recipient module.

16. The system of claim 14, wherein a different VEMM is transmitted periodically.

17. The system of claim 16, wherein a different VEMM is transmitted if said recipient module is off-line for at least a predetermined period of time.

18. The system of claim 14, further comprising a plurality of recipient modules, wherein said VEMM is unicast to each of a subset of said plurality of recipient modules.

19. The system of claim 14, further comprising a remote renewable security element for storing said subscriber key and for providing said encrypted first key and said encrypted control word to said security server.

20. The system of claim 19, wherein said subscriber key at said remote renewable security element is capable of being renewed.

21. The system of claim 19, wherein said remote renewable security element further comprises a hardware component and a software component.

22. The system of claim 21, wherein said software component determines one or more entitlements for permitting said VEMM to be generated for said recipient module.

23. The system of claim 21, wherein said hardware component encrypts said access key and said control word.

24. The system of claim 19, further comprising a plurality of said remote renewable security elements, and further comprising a broadcaster of the protected content for controlling said plurality of said remote renewable security elements.

25. The system of claim 19, wherein a plurality of said remote renewable security elements is controlled by said security server.

26. The system of claim 25, wherein said security server and said plurality of said remote renewable security elements share a server key for at least decrypting at least said access key.

27. The system of claim 26, wherein said security server generates said access key in an encrypted form as an encrypted access key, and wherein said remote renewable security element decrypts said encrypted access key to form said access key according to said server key.

28. The system of claim 19, wherein said recipient module comprises a set-top box.

29. A system for secure transmission of protected content, comprising:

(a) a remote renewable security element for encrypting a plurality of keys in a multiple key hierarchy; and

(b) a recipient module for receiving the protected content and said plurality of encrypted keys, said recipient module comprising a secret for decrypting at least one encrypted key to form a first decrypted key, said first decrypted key being required to decrypt at least one additional key in said multiple key hierarchy, wherein said recipient module is only capable of accessing the protected content with said at least one additional decrypted key in said multiple key hierarchy.

30. The system of claim 29, wherein said first encrypted key is only capable of being decrypted according to said secret.

31. The system of claim 30, wherein said recipient module comprises at least one permanent read-only storage medium for storing said secret.

32. The system of claim 31, wherein said secret is permanently stored on said at least one permanent read-only storage medium during manufacture of said recipient module.

33. The system of claim 32, wherein said recipient module comprises at least one generic chip, said at least one generic chip comprising said at least one permanent read-only storage medium for storing said secret.

34. The system of claim 33, comprising a plurality of said remote renewable security elements, and further comprising a broadcaster of the protected content for controlling said plurality of said remote renewable security elements.

35. The system of claim 29, wherein at least one of said keys in said multiple key hierarchy at said remote renewable security element is capable of being renewed.

36. The system of claim 29, wherein said remote renewable security element comprises at least one encryption mechanism.

37. The system of claim 36, further comprising a security server for receiving said first encrypted key encrypted with said secret and also for receiving said first key as an unencrypted key, such that said secret is not accessible to said security server or to said remote renewable security element.

38. The system of claim 37, further comprising a head-end for broadcasting the protected content.

39. The system of claim 38, wherein said head-end transmits an access criteria reference to said security server, and wherein said security server packages

said access criteria reference at least with said first encrypted key for transmitting to said recipient module.

40. The system of claim 39, wherein said head-end sends a EMM to said security server, for providing said access criteria reference to said security server.

41. The system of claim 40, wherein said security server constructs a VEMM from said EMM and sends said VEMM to said recipient module.

42. The system of claim 41, wherein a different VEMM is transmitted periodically.

43. The system of claim 41, wherein said security server receives an access key, encrypted with said first key, from said remote renewable security element, and wherein said security server sends said encrypted access key to said recipient module.

44. The system of claim 43, wherein said access key is not sufficient to access the protected content, and wherein said security server receives a control word, encrypted with said access key, from said remote renewable security element, and wherein said security server sends said encrypted control word to said recipient module, said control word being sufficient for said recipient module to access the protected content.

45. The system of claim 44, wherein said security server receives said control word from said head-end.

46. The system of claim 44, wherein said head-end sends at least information for generating said control word to said security server in an ECM.

47. The system of claim 46, wherein said head-end also sends said ECM to said recipient module.

48. The system of claim 47, further comprising a set-top box for receiving the protected content, said set-top box comprising a smart card located at said set-top box, said set-top box receiving said ECM and said EMM from said head-end if said set-top box is authorized to access the protected content, such that said set-top box is not required to be in communication with said security server.

49. The system of claim 39, wherein said recipient module comprises a set-top box.

50. The system of claim 49, wherein each access criteria reference is associated with a different access key.

51. A server for supporting secure transmission of protected content to a recipient module, the protected content being broadcast by a head-end, the head-end

providing an access criteria reference and a control word for accessing the protected content, the server comprising:

(a) a remote renewable security element;

(b) an entitlement message generator; and

(c) a control word message generator;

wherein said entitlement message generator receives the access criteria reference from the head-end and queries said remote renewable security element to determine whether the recipient module is entitled to receive the protected content, such that if the recipient module is entitled to receive the protected content, said entitlement message generator generates a VEMM comprising an encrypted access key and the access criteria reference; and

wherein if the recipient module is entitled to receive the protected content, said control word message generator receives the control word from the head-end and generates a VECM comprising an encrypted control word, such that the recipient module cannot access the protected content without said VEMM and said VECM.

52. A server for supporting secure transmission of protected content to a recipient module, the server comprising:

(a) a remote renewable security element for determining whether the recipient module has at least one entitlement to the protected content;

(b) a VEMM generator for generating a first message containing a first key, said VEMM generator only generating said first message if the recipient module has said at least one entitlement; and

(c) a VECM generator for generating a second message containing a second key, said second key being encrypted with said first key, wherein the protected content is only accessible according to said second key.

53. The server of claim 52, wherein the recipient module comprises a secret and said first key is encrypted, and wherein access to said first key by the recipient module is at least partially determined according to said secret.

54. The server of claim 53, wherein the recipient module receives a subscriber key encrypted with said secret from the server, and wherein said first key is encrypted with said subscriber key.

55. The server of claim 52, wherein said remote renewable security element further comprises a hardware component for encrypting said second key with said first key, and a software component for determining said entitlement.

56. A method for transmitting protected content by a broadcaster for being accessed by a subscriber, comprising:

providing a recipient module for the subscriber, said recipient module comprising a unique secret;

determining at least one access permission for said recipient module;

generating an access key to form an access message according to said access permission;

encrypting said access key to form an encrypted key, such that said secret is required to decrypt said encrypted key;

encrypting a control word with said access key to form an encrypted control word;

transmitting said encrypted key and said control word to said recipient module, wherein said recipient module requires at least said control word to access the protected content.

57. The method of claim 56, wherein each subscriber has an associated subscriber key, and wherein the broadcaster receives said subscriber key and said subscriber key encrypted with said secret to form an encrypted subscriber key, such that the broadcaster transmits said encrypted subscriber key to said recipient module as at least a portion of said encrypted key.

58. The method of claim 57, wherein said determining at least one access permission for said recipient module comprises determining an entitlement to the protected content by the subscriber.

59. The method of claim 58, wherein said encrypted access key is encrypted with said subscriber key.

60. The method of claim 59, wherein said encrypting said key with said secret to form said encrypted key further comprises constructing a VEMM, said

VEMM comprising said encrypted subscriber key, said encrypted access key and at least one access criteria reference.

61. The method of claim 60, wherein said encrypted control word is sent as part of a VECM, said VECM further comprising said at least one access criteria reference and a crypto-period index.

62. The method of claim 61, further comprising:

receiving said VEMM by said recipient module;

obtaining said access key from said VEMM with said secret and said subscriber key;

receiving said VECM by said recipient module;

obtaining said control word from said VECM with said access key; and

accessing the protected content with said control word.